International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

USING BIOMETRICS, BLOCKCHAIN AND SSI TECHNOLOGIES TO COMBAT POST REGISTRATION TRUANCY AND BUDDY PUNCHING

Edwin Ongola
Independent Scholar
Nairobi, Kenya

Abstract— **Monitoring and documenting cases of post registration truancy and "buddy punching" has been prohibitive in the past, particularly for large classes. This has been due to the potential disruption that such an exercise would cause to lesson proceedings and the lack of easy to use, non-intrusive technology to facilitate it.**
This paper presents a solution for these problems in a traditional class environment. It begins by examining student identification issues and the modern technologies available to address them. The security of both student identities and lesson attendance data is also considered, before presenting an outline of a combined solution using Biometrics, Internet of Things, Blockchain and Self Sovereign Identity technologies.
The ideas presented here can be improved upon or customized and made to work in reality. The targets of this chapter include technologists, school administrators, policy makers and academics.

Keywords— **Post Registration Truancy, Student check-in, Blockchain, Self Sovereign Identity, Internet of Things, Attendance Records, Cloud Wallets, Face Recognition**

I. INTRODUCTION

Student check-ins' are conducted for two major reasons. The first one is to try to enforce compulsory education and the second one is to try and bolster performance of individual students.
Ideally, attendance records ought to be made in a consistent manner and all pupils who come to the school premises should be recorded in some way, irrespective of their arrival or departure time (Blyth and Milner, 1999, p. 97). Usually, student-check in is conducted at the beginning of each lesson in most institutions. But this structure for monitoring attendance hides the prevalence of post-registration truancy, which according to research (van Breda, 2014), is an activity that many students around the world engage in. Post-registration truancy is when students walk out of class or school soon after registration. It should be noted that whereas official records would show that these students were present for the lesson(s), in reality they were not.
Another pertinent issue regarding attendance tracking is that, there is a need to capture why a student is absent and a distinction has to be made between authorized absence and truancy. This kind of data will usually be captured sometime after the lesson attendance was taken. Ideally the attendance data should be standardized across schools and should have the same definitions and categorizations, to ease analysis of data (Brimm and Mumpower, 2021, pp. 10-11, 17).
The paper will focus on the application of Biometrics, Blockchain and SSI, particularly to address "buddy punching" and post registration truancy.

II. IDENTIFYING STUDENTS FOR TRACKING ATTENDANCE

We are already familiar with physical student IDs. Lately, we also have digital IDs which are also referred to as virtual IDs. One of the advantages is that they can be used to access the school's online resources remotely e. g. in the case of online learning. Another key advantage is that digital ID systems can be integrated to be used with many other electronic systems (Chamera, 2024). It follows then that they can be used for attendance tracking for both in-person classes and online learning.
So a digital ID is better, however, its usage can still be improved upon by introducing multifactor authentication (MFA). Supposing we had a Two-Factor Authentication system (2FA), where besides presenting the ID, we also have to key in a password or a pin, maybe at the door before entering a class or before logging into an online class. It should be evident that both the ID and the password can willingly be shared to facilitate "buddy punching".
This brings us to a third authentication factor, biometrics.

A. Biometric registration systems –

National Research Council (2010, p. 1) defines biometrics as "the automated recognition of individuals based on their behavioral and biological characteristics." Biological

characteristics are those parts of an individual's body that are distinctive such as fingerprints, retinas, irises, facial patterns and hand geometry (Ajana, 2013). Gait recognition is an example of a behavioral characteristic (Hernandez-de-Menendez et al., 2021).

An organization that specializes in identity management, and is responsible for identities of over one billion people, declared that "There is no method or technology, other than biometrics, that can catch a person who is disclaiming his real identity" (Unique Identification Authority of India, n.d., p. 7). This justifies its inclusion in the solution.

On the surface, fingerprint scanning seems to be a great substitute for student signatures on an attendance sheet, because one student cannot check-in on behalf of another. Indeed Hernandez-de-Menendez et al. (2021) allude that the University of Sunderland, London Campus, is already making use of this technology to track class attendance.

While this is a step in the right direction, this solution would be very cumbersome to the students, if post registration truancy is to be monitored as well. This is because the students would have to register (scan their finger prints) several times, randomly, during the lesson. The situation would be worse, if the fingerprint scanner device is permanently stationed at the door, instead of being a portable one that can be passed around as one would, an attendance sheet. Most people, even the non-truants are unlikely cooperate with this activity. The system would then give the school administration the false notion that there is a high prevalence of post registration truancy.

Using iris scanning would present some of the same issues as for fingerprint biometrics.

The application of biometrics that seems most promising for attendance tracking is facial recognition. Hernandez-de-Menendez et al. (2021) describe face biometrics as fast, inexpensive, and nonintrusive. This technology is already being used by some governments for surveillance of citizens in certain public spaces.

However, data safety and privacy remains the primary concern for most would be users of biometric systems. One reason is because the data captured by biometric sensors often contains more information than may be required for identification. This may include age, sex, ethnicity and even health cues (Ross, Banerjee and Chowdhury, 2022). If irregularly obtained, this data could be used to discriminate against or target an individual. For example, insurance companies could use this kind of data to deny a person cover.

Another key concern with biometrics is that, it is difficult to stop an attacker from executing replay attacks, if he manages to steal biometric templates (Bathen et al., 2019). Indeed, the mainstream media is increasingly reporting cases of identity theft, honey-pots for hackers, toxic stores of personal identifying information, erosion of privacy, and surveillance capitalism (Zuboff, 2019).

For these reasons, biometric data has to be stored using a reasonable standard of care. Since biometric technology is a comparatively new technology, not all countries have specific laws regarding its usage. However the E.U. does, and its data privacy laws define **biometric data** as "special categories of personal data" and prohibits its "processing" (Thales, 2021) unless under specified circumstances, the key one being that the subject has given informed consent.

Nevertheless, face recognition technology has matured enough for Chen (2023) to posit that, it can be used to verify the identity of students in each class to eliminate "buddy punching" and post registration truancy.

It should be noted that a face recognition biometric system unlike other biometric systems, does not require the student to do anything regarding attendance other than to be present for the lesson. The system, after taking attendance at the beginning of a lesson, can make further attendance checks, several times, randomly, without interrupting a lesson's proceedings. Like the students, the teacher just needs to appear in class and teach, effectively saving his or her time.

B. Internet of Things (IoT) –

If we are going to employ biometric devices, particularly, face recognition cameras in a classroom, we have to network them with computers/servers, which will store the images captured (student faces), process them and do the matching in order to determine which student is present and which one is not.

Until recently, devices such as biometric scanners were not built to be part of computer networks. It is these types of devices, now able to interact with others on the internet that has given rise to the term "Internet of Things" (IoT). Rayes and Salam (2019, pp. 1-2), defines IoT devices as "a network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet".

The key concern regarding IoT, is that new types of devices are constantly coming to the fore bearing different mediums and security mechanisms, thereby making security management rather complex (The Sovrin Foundation, 2020, pp. 23-24).

Since cryptography is a primary means of securing data traversing networks, it is critical that IoT devices have cryptographic support available as a standard and not as a perk or luxury item. This would aid in the effort to reduce the security concerns within the IoT sector (The Sovrin Foundation, 2020, p. 34).

C. Where registration should be conducted –

Any identification data collected whether biometric or not, should ideally be stored in a location accessible to schools as well as relevant government education officers.

Such systems tend to be centralized with a master computer serving others. This portends a Single Point of Failure (SPoF). Whereas it may be possible to plan and mitigate problems, can centralized systems be trusted with regards to data authenticity and integrity? For example, if an administrator at a government education office were to make alterations to a student's attendance records, would it be detected ?

Our desire is a check-in system that is accurate, reliable, and authentic. We are now ready to discuss blockchain technology and how it can be used for student check-in while addressing the above questions.

III. BLOCKCHAIN TECHNOLOGY

When we talk of blockchain, we are referring to a type of Distributed Ledger Technology (DLT) where transactions are grouped into blocks and the blocks are chronologically linked together using cryptography to make records immutable (Hellwig, Karlic and Huchzermeier, 2020, pp. 4, 12).

A blockchain network is a group of peer computers where processing and storage of data is spread across the network (Lacity and Lupien, 2022, p. 42). In other words each computer in the network runs the same software and stores the exact same data (Modi, 2022, p. 13). Using consensus mechanisms the contents of the transactional ledger on the entire blockchain network is automatically synchronized. A set of protocols handle the addition of new blocks onto the chain and the selection of the valid chain (Rajbhandari, 2021, pp. 34-36).

The allure to blockchain systems and DLTs is that they are seen as a potential solution to the issue of trust. According to Lemieux and Feng (2021, pp. 1, 83, 2), in contrast to other technical systems that are built primarily for manipulation of data, blockchains are built for protection of data. These other systems are often under the control of centralized authorities and have proved to be untrustworthy. Blockchain on the other hand is said to "allow trust even if the counterparty is not known". Simply put, cryptography as used in blockchains ensures data integrity, data authenticity and non-repudiation (Hellwig, Karlic and Huchzermeier, 2020, p. 12). Moreover, the decentralized architecture of blockchain networks provides redundancy that makes them resilient to cybersecurity attacks. To compromise a blockchain network, the villain has to take control of over 50% of the processing power of all nodes on it (Lacity and Lupien, 2022, p. 42).

A. Types of blockchain networks –

There are three types of blockchains networks, namely, private blockchain, public blockchain and consortium blockchain.

Public blockchains are not owned by anyone and so any individual can join without permission from an authority. They are therefore also referred to as permissionless blockchains. Individuals are also free to select the roles their node (computer) will play on that network. For example, on some networks, an individual can sign up as a miner or a validator. Whereas miners secure the blockchain by adding blocks, validators maintain the accuracy of transactions by ensuring that only legitimate activities are processed (Kamsky, 2024). Finally, individuals running nodes on the blockchain network, can quit (remove their nodes) at any time without notice to anyone.

Private blockchains are also referred to as "permissioned" blockchains. Typically these are blockchains run by a private organization, intended for use by internal employees. For this reason, they tend to have at least one administrator. So from an administrative point of view, private blockchains are centralized (Magnuson, 2020). Private blockchains have known pre-approved end users and faster transaction times than public blockchains (Ahmed, 2020, p. 197).

A consortium blockchain is a hybrid between a private blockchain and a public blockchain where several private companies with a need to share information operate a single blockchain network. Just like with a private blockchain, a consortium blockchain will have known users and administrators. These administrators may have the powers to admit and/or eject their company nodes from the network. In a sense, a consortium blockchain is semi decentralized (Rajbhandari, 2021, pp. 71-73).

At this point we should determine whether blockchain technology would be suitable for student check-in because the technology is not always appropriate due to drawbacks like scalability, capacity, latency and privacy (Pedersen, Risius and Beck, 2019).

B. Suitability for Student check-in –

Pedersen, Risius and Beck (2019) came up with a ten-step decision path, articulated as a series of questions for determining the suitability of blockchain technology for a given project. Using those steps, I conclude that there is a valid use case for blockchain technology in a school check-in project because it can help us create a tamper-proof audit trail of attendance records in a multi-party environment (Lacity and Lupien, 2022, p. 323)

I also conclude that a public permissioned blockchain system run by a government is most suitable. In this case the public are the schools with delegation rights to their internal staff and parents.

A public permissioned blockchain system run by a government has an element of centrality to it, and is against what blockchain systems were intended to do i.e. eliminate dependence on central authorities and middle men.

Moreover, there will be a need to integrate the blockchain system with an off-chain system so that the biometric data used for recognition of students is not stored on the "check-in blockchain". This brings in the concerns mentioned earlier, because this data will likely be sitting on central servers at national level, which makes it vulnerable to large-scale hacks and data breaches (Dock labs, 2025). Is there a fix for these problems ? The answer to that question lies in Self Sovereign Identity (SSI).

IV. SELF - SOVEREIGN IDENTITY (SSI)

Lacity and Lupien (2022, p. 298) defines SSI as a decentralized and automated approach for issuing, holding, and verifying credentials.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

SSI is the third identity model after account-based and federated identity models (Preukschat and Reed, 2021, p. 7). It is a decentralized identity model, with the objective of empowering users to be in charge of their own identities and credentials. This explains the phrase "self-sovereign" (Lacity and Lupien, 2022, pp. 56, 57). The SSI identity model is more inclusive, because it is based on peer-to-peer relationships between any two entities, which cover client-server relationships as well (Reed, Preukschat and Hardman, 2021, p. 41).

In the same manner in which we carry credentials like national ID cards or insurance cards in our physical wallets, SSI technology enables the creation of digital SSI wallets in which, we can carry digital versions of our credentials. Actually, SSI technology goes a step further and provides mechanisms by which these credentials can be issued by authorized issuers and delivered directly into an entity's SSI wallet. Since the credentials are digital in nature, it is possible to receive into the SSI wallet, credentials that would otherwise not fit into a physical wallet like a University degree (Lacity and Lupien, 2022, pp. 300, 299).

A. Why use SSI for student Check-in –

As a recap, we want to automate student check-in to save time and streamline the process. At the same time we want to capture all cases regarding attendance, such as late comers or post registration truants.

We must also consider that, the education offices concerned with child welfare, are keener on absentees and not regular attendees. This drastically reduces the attendance records that need to be shared by schools.

There are no incentives for schools to keep copies of attendance records of other schools, meaning they are unlikely to be part of such a blockchain network. This leaves government education offices concerned with attendance as the only participants (node hosts). Our block chain then becomes a public permissioned blockchain with schools being the public (with write permissions). **Figure 1** shows how individual schools can have their own separate private blockchains for keeping complete attendance records, but forward absentee data to the government.

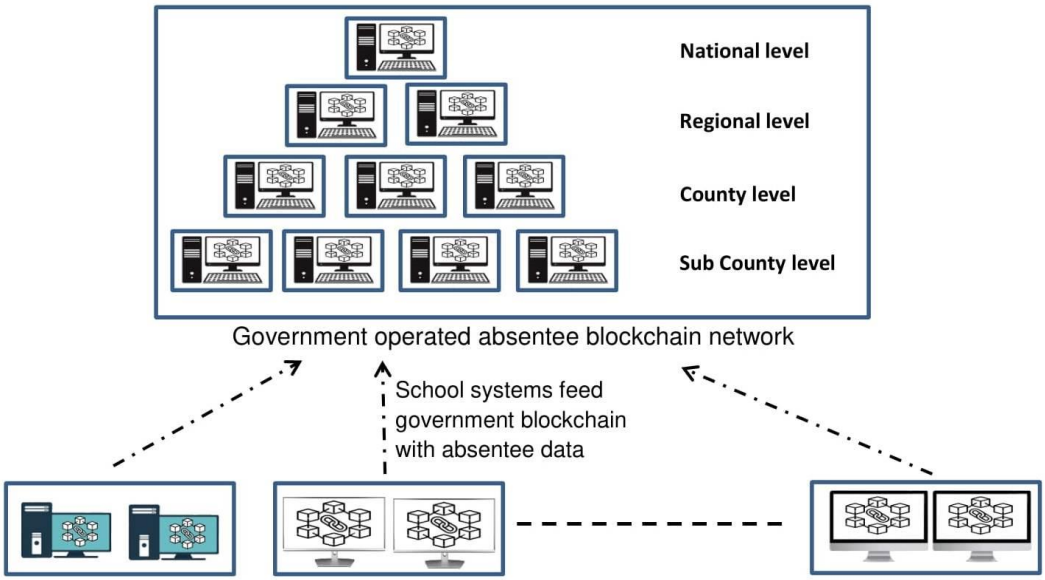

Fig. 1. Independent school operated blockchain networks for complete attendance records
(Note: The blockchain network is peer to peer. The hierarchy depicted in the diagram reflects the organization structure, not the technical implementation)

So where does SSI fit-in in all this ? The short answer is within the school, to automate check-in while protecting biometric data.

SSI provides a simple and consistent way of securing diverse IoT devices like face recognition cameras in the classrooms, and enabling them to communicate securely. Wallet agents can employ data minimization principles during the credential presentation process to avoid needless exposure of Personally Identifiable Information (PII). Moreover, SSI strongly enables GDPR compliance (The Sovrin Foundation, 2020, pp. 7, 8, 35, 31, 27).

B. Parents as guardians (guardianship credential) –

In a normal situation, it is parents who seek school admission for their children and so it makes sense for them to be a major actor in the SSI solution for student check-in.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

If an SSI solution were to be employed, we must consider that there are some students who might not be in a position to operate SSI technology devices by themselves, either due to age or the lack of a personal SSI enabled device.

Even if a policy was made requiring all students to own and carry an SSI enabled device to facilitate student check-in, the school would encounter problems with students' devices being unreachable because either the battery is dead or the students simply forgot them somewhere.

Nevertheless, attendance records would interest parents more than they would a student. This reinforces the position that parents should be major actors in facilitating the SSI based student check-in system.

It is possible to give instructions and assign responsibilities to digital agents via program code using a subclass of verifiable credentials called guardianship credentials. Using guardianship credentials, an entity can control SSI agents and wallets for another entity. The entity bestowed with this responsibility is called a digital guardian (Reed and Preukschat, 2021, p. 66).

The SSI solution for student check-in system being a concept, let's assume an environment where the presiding government not only officially recognizes verifiable credentials, but participates and acts as a governance authority. Using yet another subclass of verifiable credentials called delegation credentials, it grants some hospitals the authority to register new births with the Department of Civil Registration on behalf of parents.

So let's assume Alice gives birth to a son who she names John. When being discharged from the hospital, using her government issued SSI credential; Alice makes a request to the hospital for a birth certificate via her phone, probably initiating the transaction by scanning the hospital's QR code in the maternity wing.

Note: Figure 2 summarizes these interactions. All this takes place in less than a minute or two.

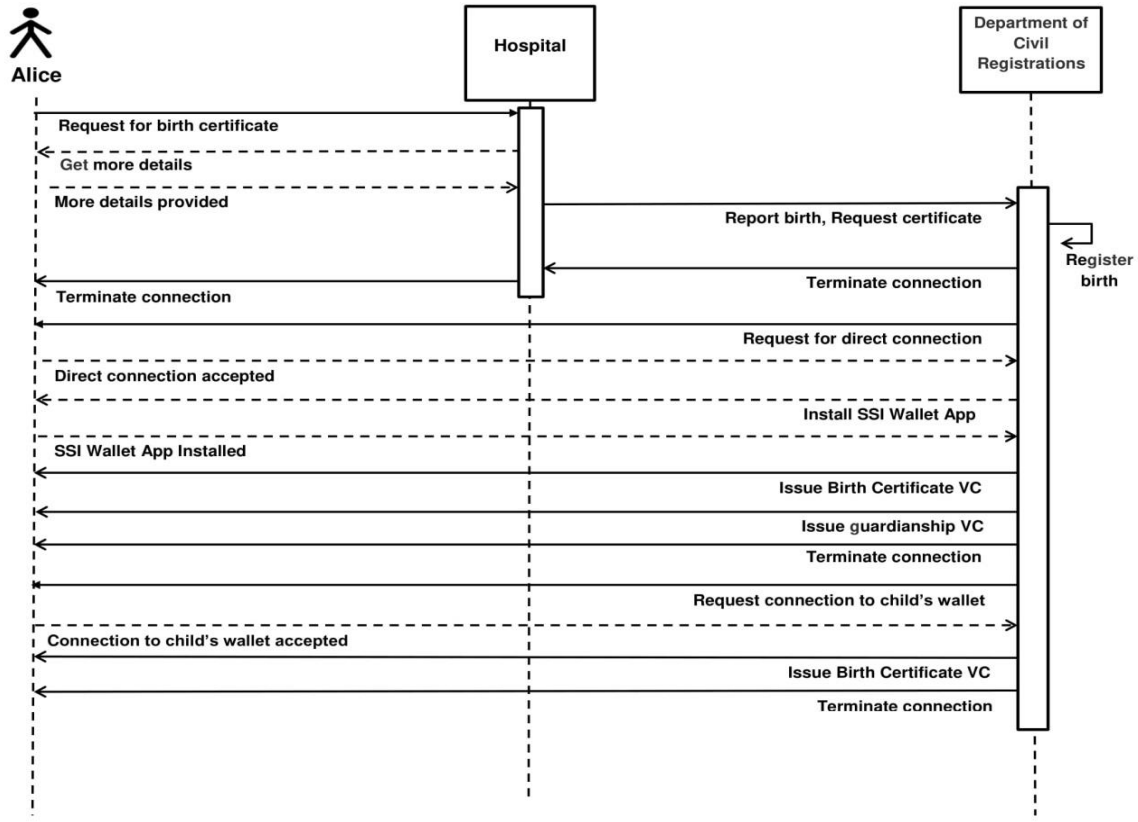

Fig. 2. A sequence diagram depicting the general SSI interactions between Alice, the hospital and the Department of Civil Registrations.

A few years later when John is ready for school, using the same process as in the hospital, Alice applies for admission at a school. In this case, some schools have been granted delegated authority by the presiding government to register new national student IDs on its behalf i.e. Department of Education. John is issued a student ID in the form of a VC, which is stored in a secure wallet belonging to John and not the school (Ruff, 2020).

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

Note: Figure 3 summarizes these interactions. All this takes place in less than a minute or two.

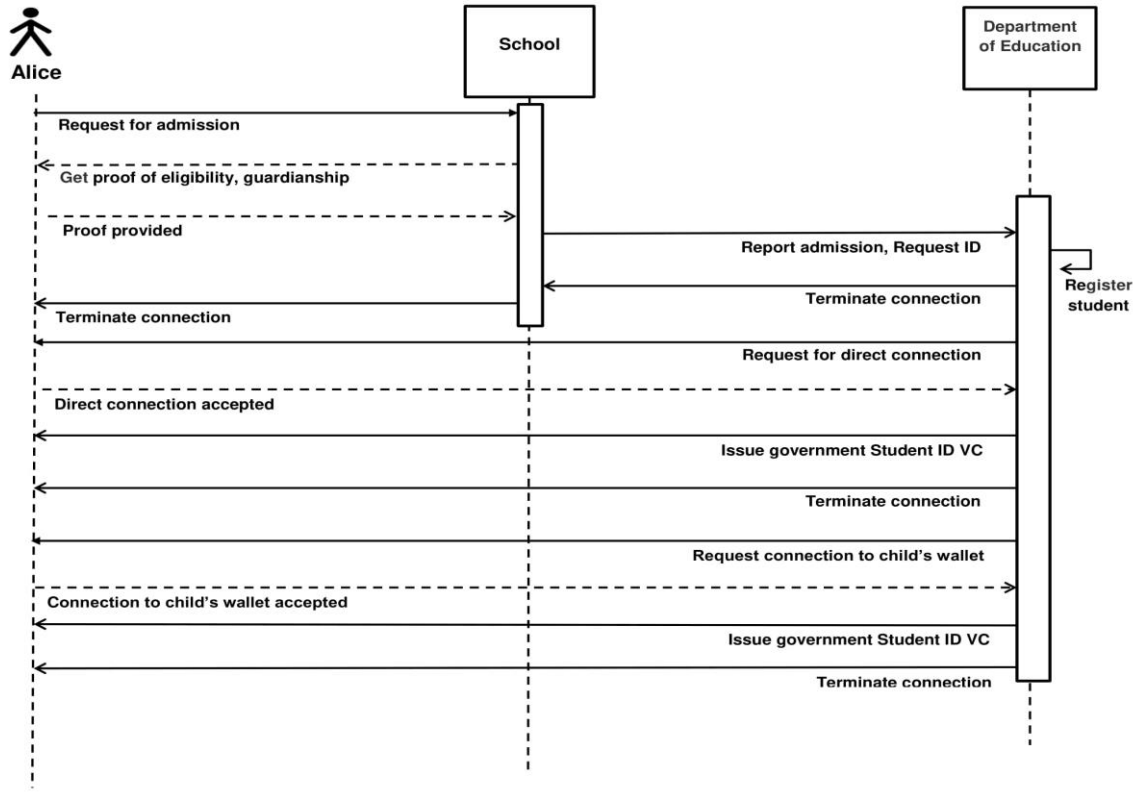

Fig. 3. A sequence diagram depicting the general SSI interactions between Alice, the school and the Department of Education.

The next setup can either take place on the same day of admission or later, but before classes begin.

To set up John's cloud wallet, to be hosted by the school's cloud agencies,

1. The school administrator initiates the transaction by generating a QR code on his/her SSI device, which Alice scans using her phone (using John's wallet).
2. School's agent also generates a new peer Decentralized Identifier (DID), only to be used with John and passes it to the John's agent. John's agent also generates a new peer DID, only to be used with the school and passes it to the school's agent (The Sovrin Foundation, 2020, pp. 20-21).
3. The school's agent registers John's current public key on the school's verifiable data registry
4. Next the school's agent requests a connection to John's wallet.
5. John accepts connection to the school's agent.
6. The school's agent prompts a sever agent to install a cloud wallet for John on a school server playing the role of a cloud agency.
7. Next, the school's agent passes the necessary information for John's agent to take charge of this cloud wallet.
8. Finally, the school's agent prompts John's agent for a facial photo of John.

This photo is not passed on to the school agent. Instead it is processed and encrypted by John's agent, then stored in John's cloud wallet within a secure data store.

In their paper about SelfI, Bathen et al. (2019) proposes the use of Cancelable biometrics to secure biometric data from being used in replay attacks. Generally, in this approach, some sort of noise is introduced or some kind of transformation is applied to the biometric data before storage. These are one way functions that cannot be reversed in theory. A similar transformation is then applied to biometric data at matching time. However, these schemes protect biometrics at the cost of sacrificing matching rates. Nevertheless, the SelfIs generation procedure as described by Bathen et al. (2019) could be applicable in our context.

9. John's agent notifies the school's agent of completion.
10. Connection between John's agent and the school's agent is terminated.

Note: The entire process takes less than a few minutes.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

Finally with the SSI architecture depicted in **Figure 4**, the school can now use SSI to track John's attendance without requiring him to do anything besides attending his lessons. This is detailed in the next section and summarized by means of a flowchart in the subsequent one.

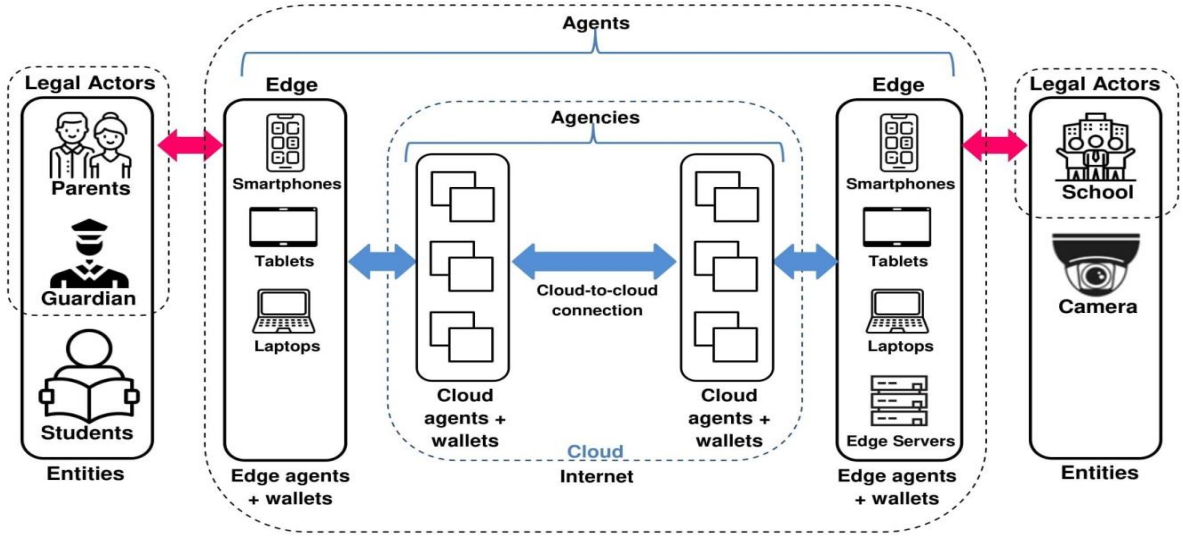

Fig. 4. An overview diagram of the role of agents and wallets in an SSI system for student check-in. Parents acting on behalf of their children, interact with the school indirectly through cloud agents operating remotely in the cloud - modified from (Reed, Joosten and van Deventer, 2021, p. 30).

C. Scenario showing how an SSI solution to Student Check-in would work –

The school being IoT enabled, has a set of networked SSI enabled face recognition cameras in every classroom and all the teachers are required to have SSI enabled devices/wallets. So student check-in is conducted in the following manner.

1. Teacher scans a camera's QR code to request connection to camera. (This camera is the lead camera in front of the class and has the capability to zoom in and out to take student photos.)
2. Lead camera's agent requests the teacher for proof of authority to use the class cameras i.e. a Verifiable Credential (VC).
3. Teacher's agent presents a VC signed by the school
4. Lead camera's agent checks the verifiable data registry to ensure that teacher's VC has not been revoked. If not, proceeds to step 5, otherwise camera sends an alert to the administration and terminates interaction with teacher's agent.
5. Lead camera's agent establishes an end-to-end connection with teacher's agent and requests for a confirmation of lesson duration after consulting the school time table agent.
6. Teacher's agent presents an interface for the teacher to confirm or adjust lesson details. Teacher's agent submits the details.

Note: Important because teachers sometimes swap lesson timings or extend/reduce their lesson durations

7. Lead camera's agent then contacts check-in agent and after verifying each other's authenticity, establishes an end-to-end connection with it.
8. Lead camera's agent then sends lesson details to check-in agent.
9. Check-in agent uses lesson details to requests for list of students registered for this lesson and their DIDs.
10. Using these DIDs, check-in agent requests for end to end connections to each of these students' cloud wallets which were created at the time of admission.

Note: Each of these connections is a Peer DID connection that provides a safe way for each student to present their photo to the Check-in agent with confidence that the other party is who they claim to be. The exchanges between two agent endpoints i.e. check-in agent & students' cloud wallets agent is called a DIDcomm exchange (The Sovrin Foundation, 2020, pp. 20-21).

11. Check-in agent creates an instance of three temporary secure data stores, which are special data containers on the network (The Sovrin Foundation, 2020, pp. 20-21).

i. adm_photos: For admission photo templates obtained from individual students' cloud wallets.

ii. checkin_pass_photos: For photos of individual students taken during a check-in pass.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

iii. lesson_photos: For photos of all students present, taken during a check-in pass.

Actually this store is a permanent parent store. Any reference to it is in fact about the child folders created at the start of a lesson (lesson folder) and the subsequent subfolders (for check-in pass folders) created during the lesson.
Each lesson folder is labeled using subject, lesson ID, date and its subfolders i.e. check-in pass folders are labeled using subject, lesson ID, date and time.
Access to lesson_photos is restricted to authorized staff members only, for dispute resolution purposes. Otherwise, lesson folders are automatically deleted after a predetermined duration, if no longer required e.g. one month.

12. Check-in agent requests each student's agent for its admission photo template and stores these in adm_photos.
13. Lead camera's agent calculates the number of student check-in passes and timings for the lesson as per lesson duration in step 6 and school policy. e.g. 5 passes @ 11:03am, then 11:10am, then 11:15am, then 11:35am, and finally at 12pm.

Note that the number of passes between the start and end of the lessons are dynamically generated for each lesson and is unknown to either the teacher or the student.

14. Lead camera's agent checks the verifiable data registry for DID addresses of other authorized cameras within the class (slave cameras), and establishes end-to-end connections with them i.e. there are no intermediaries, thus making the connections secure.
15. Lead camera's agent synchronizes its clock with the slave cameras.
16. Lead camera's agent shares student check-in times for the lesson. (So that they are all taking class photos at the same time.)

Note: Slave cameras don't scan faces. They take one photo of everyone present in a given check-in pass. They are stationed at the sides and back of the classrooms to provide different views of attendees. The output of the slave cameras goes to the lesson_photos data store.

17. At the predetermined time, Lead camera and slave cameras' agents simultaneously take lesson photos covering all students.
18. The slave camera's agents time stamp, digitally sign and forward these to the lead camera
19. Immediately after taking a lesson photo, the lead camera's agent directs the lead camera to scan and take photos of faces of present students, one after the other in quick succession.

Note that there are products in the market that claim accuracy rates as high as 99.87% and also claim to be able to recognize a face on live video in less than 100 milliseconds (RealNetworks, n.d.). It is should be possible to accomplish this task in less than one minute, even for a class of 200 students.

20. Lead camera's agent forwards lesson photos from itself and slave cameras to the check-in agent.
21. Check-in agent places lesson photos in lesson_photos store
22. Lead camera's agent forwards individual face photos to check-in agent.
23. Check-in agent places individual face photos in checkin_pass_photos store
24. Check-in agent compares each of the photos from checkin_pass_photos store to the photos in the adm_photos store.

Note: The same transformation similar to the one done to the data in the adm_photos store has to be done to those in the checkin_pass_photos store prior to comparison. If there is a match, the check-in agent records who was present and the time in a **Lesson attendance log** such as depicted in **Table 1**.

25. End of check-in pass - contents of checkin_pass_photos are cleared.

Table -1 Lesson attendance log

DID	11:03 am	11:10 am	11:15 am	11:55 am	12:00 pm	CSC	DPR (%)
did1	1	1	1	1	1	1	100
did2	0	1	1	1	0	4	80
did3	0	0	0	0	0	0	0
did4	1	0	0	0	1	5	40
……	…….	……	….	….	….	..…	…
did25	1	1	1	1	1	1	100

The values for CSC column i.e. check-in Status Code, are derived from **Table 2**.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

In **Table 1**, did1 (student1), is fully present, did2 (student2) came late and left early, did3 (student3) was completely absent, and did4 (student4) was present at the beginning and end of the lesson, but mostly absent in between.
The last column DPR%, i.e. Detected Presence Rate is a simple calculation of the number of times a student is detected over the number of times check-in is done multiplied by 100. DPR (%) is important because it makes it possible to work out the overall percentage detections of a face (student) over a given duration e.g. 70% attendance in geography in term I. If a student is below the required attendance rate, his cloud wallet can send him or his guardian an alert encouraging him to stay in class longer. Both CSC and DPR(%) need not be stored because they can always be derived from the other columns.

Table -2 Check-in Status Codes

Check-in Status	**CSC**
Fully present	1
Fully absent	0
Present but came in late and stayed on until end	2
Came in early and left early	3
Came in late and left early	4
Irregular (was present at the beginning and end of the lesson, but mostly absent in between	5

Note: Steps 17 to 25 are carried out repeatedly until the last check-in pass has been processed.
Some mechanism could be added that allows the teacher to either prematurely terminate or extend the lesson by interacting with the lead camera's agent as per step 5 & 6. Terminating the lesson early would imply replacing the pending check-in passes with one last one after processing the update. Extending it would imply adding more check-in passes beyond the last one (it would certainly be helpful if a teacher can get an alert e.g. 5 minutes before the last check-in pass). Whatever the case, after the last check-in pass has been processed, step 26 comes next.

26. Check-in agent sends lesson attendance log to the school's check-in blockchain where it cannot be tampered with.

Note: Government's absentees blockchain can receive delayed updates because the reasons for absence must be determined first.

27. Check-in agent also sends to each DID (student) a signed copy of their attendance information to be stored in their cloud wallet (can later be imported into their edge devices) e.g. student 1 and student 4's data could contain the following information as shown in **Figure 5**.

DID	did1
Subject ID	UCU102
Lesson ID	05
Date	17-02-2025
11:03	1
11:10	1
11:15	1
11:35	1
12:00	1
Timestamp	12:02
Issuer	Students' check-in agent's digital signature

DID	did4
Subject ID	UCU102
Lesson ID	05
Date	17-02-2025
11:03	1
11:10	0
11:15	0
11:35	0
12:00	1
Timestamp	12:02
Issuer	Students' check-in agent's digital signature

Fig. 5. Lesson attendance information

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 15-26
Published Online April 2025 in IJEAST (http://www.ijeast.com)

These serve as attendance micro credentials or preliminary attendance credentials that will be replaced by a single verifiable credential for attendance, detailing overall Detected Presence rate for each subject.

28. Lead camera's agent terminates connection with teacher's agent.
29. Lead camera's agent terminates connection with slave camera's agent.
30. Lead camera's agent terminates connection with check-in agent.
31. Check-in agent deletes instance of checkin_pass_photos.
32. Check-in agent deletes instance of adm_photos.

The above steps are summarized in the flowchart shown in **Figure 6**.

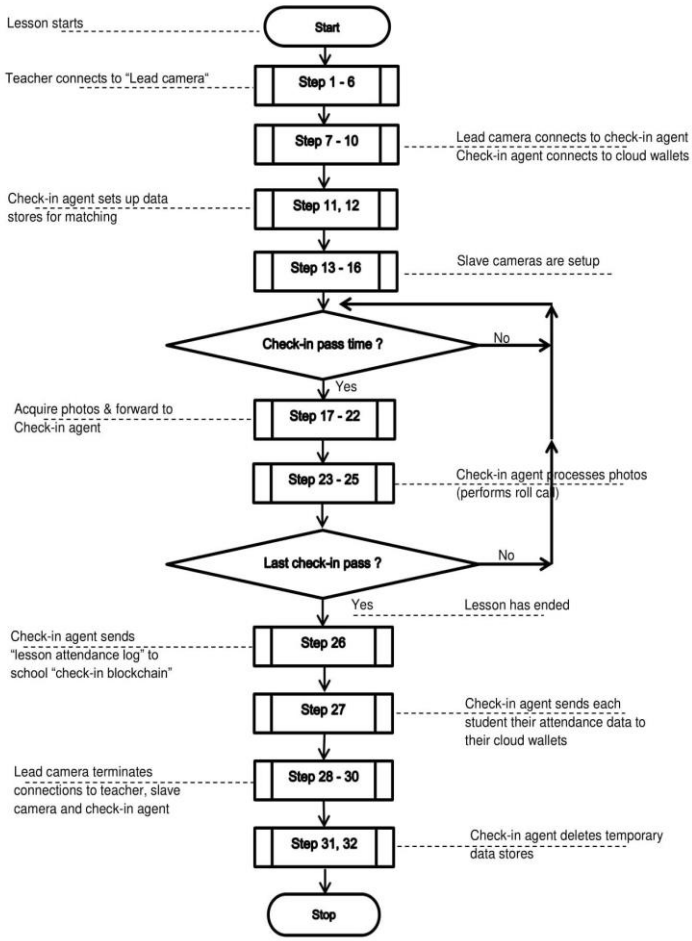

Fig. 6. Flowchart showing the general steps for conducting student check-in using SSI

V. DISCUSSION

The proposed SSI solution to student check-in allows the collection of attendance information in a uniform manner and therefore makes it easy to generate statistical information about individual students or groups of students for any time periods.

Using smart contracts in a school's "check-in blockchain", class attendance can be monitored and certificates can be automatically generated at the conclusion of a course. Depending on an institutions policy, certificates can be used to determine eligibility to sit for examinations.

The proposed system solves huge problems regarding post registration truancy and irregular attendance while making it possible and easy for guardians to monitor their children's attendance.

In cases of attendance disputes, it provides photo evidence to aid in satisfactory resolution.

From a technical perspective, it provides an attractive solution for the security of biometric data. Finally, the proposed system comes with some unintended benefits too. Teachers will be a bit more careful about their own attendance and how long they conduct their classes. Secondly, class discipline could be

enhanced because no one knows when a check-in pass is occurring. All this is made possible without cumbersome wearable devices or dreaded chip implants.

However, does the proposed SSI solution to student check-in generate enough value so that it will likely to be adopted? (Lacity and Lupien, 2022, p. 411). According to Lacity and Lupien (2022, p. 418), there are five attributes that make people want to adopt innovations. These are relative advantage, trial-ability, compatibility, observability, and complexity. The proposed system has these attributes, however unless some additional school & student management features are incorporated, the system might be too costly for most schools. Apart from that, SSI is an ecosystem play and ecosystems are hard and slow to build (Lacity and Lupien, 2022, p. 329), particularly without government support. Fortunately, in this case, if a school wanted to implement this system, it is possible to do so and gain the same benefits without government involvement – only teachers, students and parents would require Self Sovereign Identities issued by the school, rather than the government.

Current technological advancements in AI, blockchain, biometrics and SSI point to future where the learning environment will be more personalized. Indeed online classes are already common place. So schools requiring physical presence of the student will be reduced, particularly if the courses' practical components do not require an expensive lab set up. The proposed SSI solution to student check-in would still work for remote students albeit with minor adjustments.

Also, student check-in done to coerce students to attend classes with the expectation that their attendance will correlate with performance, does not work in all cases. Merely being present on its own, does not necessarily improve learning (Sekiwu, 2020). In some technology-based instruction systems, assessments are closely woven into learning activities in an unobtrusive manner. This forces the learner to personally engage with the content so that they can rate well in assessments. In such systems it is possible to track progress through the content (check-in) and also how well the content was understood through micro assessments (learning). A student posting poor results in these assessments may be forced to relearn and retake a test before progressing to the next level. Such systems are already being used for some online courses.

VI.CONCLUSION

Blockchain technology despite its recent hype is not a solution for all problems. In the long term, blockchain & SSI will be used in the education sector primarily for provenance of evidence of an individual's learning. SSI in particular will be used for presentation and verification of proof of that learning.

VII. REFERENCE

[1] Blyth, E. and Milner, J. (1999). Improving school attendance. London ; New York: Routledge, p. 97.

[2] van Breda, M. (2014). School Truancy: Poor School Attenders' Perceptions of the Impact Regarding Dysfunctional Teacher-Learner Relationships on Truant Behaviour. Mediterranean Journal of Social Sciences, [online] 5(23). doi:https://doi.org/10.5901/mjss.2014.v5n23p1056.

[3] Brimm, D. and Mumpower, J.E. (2021). Student Attendance in Tennessee. [online] comptroller.tn.gov. Nashville, Tennessee: OREA, pp. 10-11, 17. Available at: https://comptroller.tn.gov/content/dam/cot/orea/advanced-search/2021/StudentAttendanceReport.pdf [Accessed 7 Mar. 2025].

[4] Chamera (2024). Benefits of Choosing Digital Student ID Cards. [online] Chamera. Available at: https://www.chamera.com/top-reasons-to-switch-to-digital-student-id-cards/ [Accessed 24 Jan. 2025].

[5] National Research Council (U.S.) (2010). Biometric Recognition: Challenges and Opportunities. Washington, D.C.: National Academies Press, p.1.

[6] Ajana, B. (2013). Asylum, Identity Management and Biometric Control. Journal of Refugee Studies, 26(4), pp.576–595. doi:https://doi.org/10.1093/jrs/fet030.

[7] Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C.A. and Arinez, J. (2021). Biometric applications in education. International Journal on Interactive Design and Manufacturing (IJIDeM), [online] 15(2-3), pp.365–380. doi:https://doi.org/10.1007/s12008-021-00760-6.

[8] Unique Identification Authority of India (n.d.). Role of Biometric Technology in Aadhaar Enrollment. [online] New Delhi: UIDAI, p.7. Available at: http://www.dematerialisedid.com/PDFs/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf [Accessed 19 Nov. 2024].

[9] Ross, A., Banerjee, S. and Chowdhury, A. (2022). Deducing health cues from biometric data. Computer Vision and Image Understanding, 221, p.103438. doi:https://doi.org/10.1016/j.cviu.2022.103438.

[10] Bathen, L., Flores, G.H., Madl, G., Jadav, D., Arvanitis, A., Santhanam, K., Zeng, C. and Gordon, A. (2019). SelfIs: Self-Sovereign Biometric IDs. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), [online] pp.2847–2856. doi:https://doi.org/10.1109/cvprw.2019.00344.

[11] Zuboff, S. (2019). AGE OF SURVEILLANCE CAPITALISM: The fight for a human future at the new frontier of power. S.L.: Public Affairs.

[12] Thales (2021). Biometric data protection (EU and US perspectives). [online] www.thalesgroup.com. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data [Accessed 27 Jan. 2025].

[13] Chen, X. (2023). Study on Student Attendance System Based on Face Recognition. Journal of physics, 2492(1), pp.012015–012015. doi:https://doi.org/10.1088/1742-6596/2492/1/012015.

[14] Rayes, A. and Salam, S. (2019). Internet of Things from hype to reality: the road to digitization. Cham, Switzerland: Springer, pp. 1-2.

[15] The Sovrin Foundation (2020). Self-Sovereign Identity and IoT (A whitepaper on the security opportunities and business potential for self-sovereign identity with the Internet of Things). pp. 7, 8, 20-21, 23-24, 27, 31, 34, 35

[16] Hellwig, D., Karlic, G. and Huchzermeier, A. (2020). Build Your Own Blockchain. Switzerland: Springer International Publishing, pp.4, 12.

[17] Lacity, M.C. and Lupien, S.C. (2022). Blockchain Fundamentals for Web 3.0. University of Arkansas Press, pp. 42, 56, 57, 299, 300, 323, 329, 411, 418.

[18] Modi, R. (2022). Solidity Programming Essentials. 2nd ed. Packt Publishing Ltd, p. 13.

[19] Lemieux, V.L. and Feng, C. eds., (2021). Building Decentralized Trust. Springer Nature, pp. 1, 83, 2.

[20] Rajbhandari, R. (2021). A book about blockchain : how companies can adopt public blockchain to leap into the future. New York, New York (222 East 46th Street, New York, NY 10017): Business Expert Press, pp. 34-36, 71-73.

[21] Ahmed, M. ed., (2020). Blockchain in data analytics. Newcastle Upon Tyne: Cambridge Scholars Publishing, p. 197.

[22] Kamsky, A. (2024). Mining Bitcoin vs. Validating Bitcoin Transactions: Key Differences Explained. [online] ccn.com. Available at: https://www.ccn.com/education/crypto/bitcoin-mining-vs-transaction-validation/ [Accessed 3 Feb. 2025].

[23] Magnuson, W. (2020). Blockchain Democracy: Technology, Law and the Rule of the Crowd. Cambridge University Press, p. 203.

[24] Pedersen, A.B., Risius, M. and Beck, R. (2019). A Ten-Step Decision Path to Determine When to Use Blockchain Technologies. MIS Quarterly Executive, [online] 18(2), p. Article 3. doi:https://doi.org/10.17705/2msqe.00010.

[25] Dock labs (2025). Self-Sovereign Identity: The Ultimate Guide 2024. [online] www.dock.io. Available at: https://www.dock.io/post/self-sovereign-identity [Accessed 6 Feb. 2025].

[26] Preukschat, A. and Reed, D. (2021). Why the internet is missing an identity layer—and why SSI can finally provide one. In: Self-Sovereign Identity DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS. Shelter Island: Manning Publications Co, p. 7.

[27] Reed, D., Preukschat, A. and Hardman, D. (2021). Example scenarios showing how SSI works. In: Self-Sovereign Identity DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS. Shelter Island: Manning Publications Co, p. 41.

[28] Reed, D., Joosten, R. and van Deventer, O. (2021). The basic building blocks of SSI. In: Self-Sovereign Identity DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS. Shelter Island: Manning Publications Co, p. 30.

[29] Dock Labs (2025). Verifiable Credentials: The Ultimate Guide 2024. [online] www.dock.io. Available at: https://www.dock.io/post/verifiable-credentials [Accessed 12 Feb. 2025].

[30] Reed, D. and Preukschat, A. (2021). SSI Scorecard: Major features and benefits of SSI. In: Self-Sovereign Identity DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS. Shelter Island: Manning Publications Co, p. 66.

[31] Ruff, T. (2020). Introducing Self-Sovereign Student ID - Timothy Ruff - Medium. [online] Medium. Available at: https://rufftimo.medium.com/introducing-self-sovereign-student-id-part-2-of-2-a566ed414d75 [Accessed 18 Feb. 2025].

[32] RealNetworks (n.d.). The Best-Performing Face Recognition for Live Video . [online] https://safr.com. RealNetworks. Available at: https://safr.com/wp-content/uploads/2020/03/SAFRSecurity_022820.pdf [Accessed 18 Feb. 2025].

[33] Sekiwu, D. (2020). Investigating the relationship between school attendance and academic performance in universal primary education: The case of Uganda. African Educational Research Journal, [online] 8(2), pp.152–160. doi:https://doi.org/10.30918/aerj.82.20.017.